UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,694	10/31/2001	Richard L. Schertz	10017330-1	4657

7590 09/27/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,694	SCHERTZ ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 06/23/06.

2. Claims 1-23 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 6-9, 11, 14-16, 18, and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al, US/6347374 (Cited in PTO dated 03/23/06), hereinafter "Drake", in view of Ethereal, http://web.archive.org/web/20001109065300/www.ethereal.com/introduction.html dated 11/09/2000.

5. As per claims 1, 9, and 16:

Drake teaches "A method of presenting data related to an intrusion event on a computer system, comprising:

capturing data related to the intrusion event" in (Col 3 lines 18-25, Col 5 lines 38-45, Col 7 lines 45-53);

"decoding the captured data from a predetermined format to a predetermined format (normalized format) decipherable by humans" in (Col 5 line 60 to Col 6 line 67), "the decoded data in turn comprises data summary, and detailed data; and

presenting the decoded data to a user in an organized manner" in (Col 6 line 20 to Col 7 line 10) .

However, Drake does not specifically discloses "determining at least one data component of the presented decoded data that is related to another data component of the presented decode data; and

graphically identifying the at least one data component of the presented decoded data".

Nevertheless, Ethereal discloses ""determining at least one data component of the presented decoded data that is related to another data component of the presented decode data; and

graphically identifying the at least one data component of the presented decoded data" see (Picture mainwin-19990804.gif) [The picture shows a feature of selecting an event (e.g. No. 35 in the top window graphic interface) to decode the event data showing in the second window. As desired, the user can select a first data component (e.g. "Destination: ethereal (206.57.36.90)) of one of the presented decoded data that is related to another data component of the presented decoded data; and graphically identifying (highlighting in bold letter in the third windows) the at least one data

component of the presented decoded data (displaying the hexadecimal format of the data "**CE 39 24 5A ..... .9$Z.**"

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's teaching to incorporate the feature "determining at least one data component of the presented decoded data that is related to another data component of the presented decode data; and

graphically identifying the at least one data component of the presented decoded data" to allow the user graphically identify the decoded data and relationship of the decoded data to its original undecoded format event data for faster recognition of the intrusion event.

6. As per claim 2:

Drake teaches "The method, as set forth in claim 1, wherein capturing data comprises capturing network data packets of the intrusion event" in (Col 7 lines 45-53).

7. As per claims 3, 11, and 18:

Drake teaches "The method, as set forth in claims 1, 9, and 16, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format" in (Col 8 lines 1-10, and Col 5 line 60 to Col 6 line 20).

8. As per claims 6 and 21:

Drake teaches "The method, as set forth in claims 1 and 16, wherein presenting the decoded data comprises displaying the decoded data on a computer screen" in (Col 17 lines 1-25).

9. As per claims 7, 14, and 22:

Drake teaches "The method, as set forth in claims 1, 9, and 16, wherein presenting the decoded data comprises graphically displaying the decoded data according to a predetermined report organization and format" in (Col 17 lines 50-60).

10. As per claims 8,15, and 23:

Drake teaches "The method, as set forth in claims 1 and 16, wherein presenting the decoded data comprises generating a report having the decoded data" in (Col 17 lines 50-60).

11. As per claim 9:

Drake teaches "A method of presenting data related to an intrusion system, comprising:

Capturing, from a network, data related to the intrusion event in response to a trigger" in (Col 3 lines 18-25, Col 5 lines 38-45, Col 7 lines 45-53);

"decoding the captured data from a first predetermined format to a second predetermined format (normalized format)" in (Col 5 line 60 to Col 6 line 67), "the decoded data in turn comprises data summary, and detailed data; and

presenting the decoded data according to a predetermined report format" in (Col 6 line 20 to Col 7 line 10) ;

receiving user input graphically highlighting a first data component of the presented decoded data;

determining at least one other data component of the presented decoded data that is related to the first data component; and

graphically highlighting the at least one other data component of the presented decoded data.

However, Drake does not specifically discloses "receiving user input graphically highlighting a first data component of the presented decoded data;

determining at least one other data component of the presented decoded data that is related to the first data component; and

graphically highlighting the at least one other data component of the presented decoded data.".

Nevertheless, Ethereal discloses ""receiving user input graphically highlighting a first data component of the presented decoded data;

determining at least one other data component of the presented decoded data that is related to the first data component; and

graphically highlighting the at least one other data component of the presented decoded data." see (Picture mainwin-19990804.gif) [The picture shows a feature of selecting an event (e.g. No. 35 in the top window graphic interface) to decode the event data showing in the second window. As desired, the user can select a first data component (e.g. "Destination: ethereal (206.57.36.90)) of one of the presented decoded data that is related to another data component of the presented decoded data; and graphically identifying (highlighting in bold letter in the third windows) the at least one data component of the presented decoded data (displaying the hexadecimal format of the data "**CE 39 24 5A ..... .9$Z.**"

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's teaching to incorporate the feature "receiving user input graphically highlighting a first data component of the presented decoded data;

determining at least one other data component of the presented decoded data that is related to the first data component; and

graphically highlighting the at least one other data component of the presented decoded data." to allow the user graphically identify the decoded data and relationship of the decoded data to its original undecoded format event data for faster recognition of the intrusion event.

12. As per claim 16:

Drake discloses "A system of presenting data of an intrusion detection system, comprising:

A network driver capturing data related to an intrusion event from a network;

A decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising intrusion event data, data summary, and detailed data;

A mapping table that correlates related data components of the decoded intrusion event data, data summary and detailed data; and

A user interface presenting the decoded data to a user, wherein the user interface is operable, responsive to receiving user input selecting a first data component of one of the presented decoded intrusion event data, data summary and detailed data, to graphically identify any data components of the others of the presented decoded intrusion event data, data summary and detailed data that the mapping table correleates to the first data component.

However, Drake does not specifically discloses "A mapping table that correlates related data components of the decoded intrusion event data, data summary and detailed data; and

A user interface presenting the decoded data to a user, wherein the user interface is operable, responsive to receiving user input selecting a first data component of one of the presented decoded intrusion event data, data summary and detailed data, to graphically identify any data components of the others of the presented decoded intrusion event data, data summary and detailed data that the mapping table correleates to the first data component."

Nevertheless, Ethereal discloses "A mapping table that correlates related data components of the decoded intrusion event data, data summary and detailed data; and

A user interface presenting the decoded data to a user, wherein the user interface is operable, responsive to receiving user input selecting a first data component of one of the presented decoded intrusion event data, data summary and detailed data, to graphically identify any data components of the others of the presented decoded intrusion event data, data summary and detailed data that the mapping table correleates to the first data component." see (Picture mainwin-19990804.gif) [The picture shows a feature of selecting an event (e.g. No. 35 in the top window graphic interface) to decode the event data showing in the second window. As desired, the user can select a first data component (e.g. "Destination: ethereal (206.57.36.90)) of one of the presented decoded data that is related to another data component of the presented decoded data; and graphically identifying (highlighting in bold letter in the third windows) the at least one data component of the presented decoded data (displaying the hexadecimal format of the data "**CE 39 24 5A ..... .9$Z.**"

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's teaching to incorporate the feature "A mapping table that correlates related data components of the decoded intrusion event data, data summary and detailed data; and

A user interface presenting the decoded data to a user, wherein the user interface is operable, responsive to receiving user input selecting a first data component of one of the presented decoded intrusion event data, data summary and detailed data,

to graphically identify any data components of the others of the presented decoded intrusion event data, data summary and detailed data that the mapping table correleates to the first data component." to allow the user graphically identify the decoded data and relationship of the decoded data to its original undecoded format event data for faster recognition of the intrusion event.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 4-5, 10, 12-13, 17, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drake in view of Baker, US/6775657.

15. As per claims 4-5, 12-13, and 19-20:

Drake teaches "The method, as set forth in claims 1, 9, and 16. However, Drake is silent on the "decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format". Nevertheless, Baker discloses the "Multilayered Intrusion Detection System and Method" invention, which includes a method of capture the data packet having a data

link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format in (Col 4 lines 40-46). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's invention to incorporate Baker's teaching to add more detail information about the network data.

16. As per claims 10 and 17:

Drake teaches "The method, as set forth in claims 9 and 16". However, Drake is silent on "capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined signature in the network data packet". Nevertheless, Baker does disclose a method of capturing data and detecting the presence of a predetermined signature in the network data packet (Col 5 line 45 to Col 6 line 9). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Drake's invention to incorporate Baker's teaching to include another method of detecting the network intrusion in real time.

Response to Arguments

17. Applicant has amended claims 1, 9, and 16, which necessitated new grounds of rejection. See Rejections above.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100